Revista Latina de Sociología

Revista Latina de Sociología (RELASO)
Vol. 8(2) (2018) pp. 23-33. ISSN-e 2253-6469
DOI:https://doi.org/10.17979/relaso.2018.8.2.2951

Entre Huxley y Orwell: Big Data y salud

Between Huxley and Orwell: Big Data and Health

Jorge Alberto Álvarez Díaz
Universidad Autónoma Metropolitana Unidad Xochimilco, México
bioetica_reproductiva@hotmail.com

Eduardo Alfredo Duro
Facultad de Ciencias de la Salud, Universidad de Morón, Argentina
eaduro@hotmail.com

Ida Cristina Gubert
Comité de Ética en Investigación, Universidad Federal de Paraná, Brasil
gubertida@gmail.com

Carmen Alicia Cardozo de Martínez
Facultad de Ciencias Químicas y Farmacéuticas, Universidad de Chile, Chile
carmen_aliciademartinez@yahoo.co.uk

María Angélica Sotomayor
Comité de Ética, Universidad de Santiago de Chile, Chile
masotomay@gmail.com

Luis López
Facultad de Ciencias Médicas, Universidad de San Carlos de Guatemala, Guatemala
ensayos.clinicos@gmail.com

Alejandro Duro
Instituto Tecnológico y de Estudios Superiores de Monterrey, Argentina
alejandroduro@yahoo.com.ar

Rosa Niño Moya
Facultad de Medicina, Universidad de Chile, Facultad de Salud y Odontología, Universidad Diego Portales, Chile
rninomoya@hotmail.com

Patricia Sorokin
Facultad de Medicina, Universidad de Buenos Aires, Argentina
patriciasorokin@gmail.com

Recibido/Received: 30/08/2017
Aceptado/Accepted: 13/01/2018

RESUMEN:
Cuando en el año 1966 Naciones Unidas planteaba en su Declaración Internacional de los Derechos Civiles y Políticos, el ideal de un ser humano libre con respeto a su intimidad a través de la prohibición de injerencias arbitrarias en su vida privada, no era posible imaginar el impacto global que tendría la irrupción de una conectividad casi ilimitada, la autonomía de las nuevas tecnologías de la información, el desarrollo de enormes bases de datos interconectadas, la circulación independiente e irrestricta de datos, que han generado interrogantes éticos y jurídicos derivados de esta forma de tratar los datos personales y de salud
Palabras clave: Big Data; Internet; Salud; Ética; Intimidad; Seguridad

ABSTRACT:
When in 1966 the United Nations stated in its International Covenant on Civil and Political Rights, the ideal of a free human being with respect to his privacy through the prohibition of arbitrary interference in his private life, it was not possible to imagine the impact of global unlimited connectivity, autonomy of new information technologies, the development of huge interconnected databases, the independent and unrestricted circulation of data, which have led to ethical and legal questions arising from this to treat personal and health data.

Keywords: Big Data; Internet; Health; Ethics; Privacy; Security

Introducción: del ritual de la confesión al ritual del clic

El Señor K se levanta por la mañana y tras ducharse acude a tomarse un café en un sitio novedoso. Inicia una aplicación de su teléfono móvil para que le indique el rumbo. Al llegar aprovecha la espera entrando a su servicio electrónico de banca en línea para realizar algunos pagos antes de hacer el pago de su tarjeta de crédito. Revisa en una tienda en línea algunos títulos de libros. Llega ese amigo que tenía tiempo de no ver, y para compartir el gusto se toman una fotografía que suben a una red social (enlazada a otras dos más). Al aparecer la fotografía el servicio les sugiere los nombres de ambos por reconocimiento facial. Ambos utilizan algunos minutos para responder los primeros comentarios de amistades comunes en redes sociales. Hacia el final de la charla, el Señor K entra nuevamente en su teléfono móvil para confirmar la cita médica de la siguiente semana y revisar si ya le hicieron el pago de su nómina (que no se había reflejado en la revisión anterior). Ya aparecía. Todos, al igual que el Señor K, nos encontramos inmersos en el *Big Data.*

El término "*Big Data*" no tiene una traducción consensuada en la lengua española; se ha traducido por "macrodatos", "datos masivos", "datos a gran escala", etc. Tal vez lo adecuado, dada la falta de consenso, sea dejar el término en lengua inglesa y así trabajar mientras no ocurre alguna cosa más. El término de *Big Data* se popularizó con John Mashey (1999) a finales del milenio pasado, en una conferencia para USENIX (*The Advanced Computing Systems Association*). Allí hablaba del estrés que sufrirían las infraestructuras físicas y humanas de la informática como consecuencia del imparable (y al parecer, inevitable) aumento en los datos. Pudo otear en el horizonte lo que al día de hoy es una realidad. La red social Facebook se fundó en 2004; según datos de Wikipedia, a marzo de 2017 contaba con 1.94 mil millones de usuarios, dando servicio con una red de 50'000 servidores. Podría seguirse un listado interminable de sitios que reciben millones de visitas por día.

Así, el *Big Data* se refiere al tratamiento masivo de datos: su recolección, almacenaje, análisis, clasificación y utilización de esa cantidad inmensa de información. De ahí que hay quien habla de las "tres V" del *Big Data*: volumen, velocidad y variedad. La gestión de ese volumen descomunal de datos, cada vez a mayores velocidades, y con una extraordinaria variedad, hace que la reflexión sobre el tema no se trate de algo menor. Como puede apreciarse, el tema toca prácticamente todas las aristas de la vida humana; al ser tan abarcante, el propósito de este trabajo es reflexionar acerca del *Big Data* en salud, y específicamente, de la problemática bioética que subyace al tema.

De la utopía a la distopía

El uso de telefonía móvil es ahora cosa cotidiana para cada vez más gente. Una cantidad enorme de aplicaciones funciona gracias a los datos que puede emitir una tarjeta SIM (acrónimo en inglés de "*subscriber identity module*"). No están solamente entre los nórdicos o exclusivamente en países desarrollados; los países menos desarrollados las tienen, y desde Sierra Leona hasta Latinoamérica se dispone de ellas, aunque sea de las denominadas de gama baja. Las tarjetas SIM permiten localizar al usuario del teléfono, de modo que al combinarse con datos satelitales es posible seguirle incluso en tiempo real (cualquier usuario de servicios de geolocalización, como GPS, maps, etc. ha vivido esto). Esto ha permitido que personas con un teléfono móvil pongan sobre el mapa poblados que no se tenían ubicados. En 2010, tras el terremoto en Haití, fue posible localizar a mucha gente que migró, y al ubicarla, fue posible diseñar algunas estrategias para el auxilio. Se ha pensado en "ciudades inteligentes", donde se pueda aplicar este tipo de innovaciones para intentar solucionar problemas de tráfico, transporte público, seguridad, etc.

Registros de las palabras clave elegidas por los usuarios y la información de la localización de sus direcciones IP, proporcionados por motores de búsqueda comerciales, fueron analizados como un método de bajo costo para conocer la epidemiología de algunas enfermedades y su comportamiento en el hábitat. (Ginsberg J, Mohebbi MH, Patel RS, Brammer L, Smolinski MS, Brilliant L, 2009) (Polgreen PM, Chen Y, Pennock DM, Nelson FD, 2008)

Trabajos en revistas indexadas promueven llevar adelante, incluso establecer vigilancia epidemiológica sobre las publicaciones en las redes sociales. Se están desarrollando algoritmos que pueden interactuar con las redes para conocer, por ejemplo el estado de ánimo de las personas conectadas en las redes (Gruebner O, Sykora M, Lowe SR, Shankardass K, Galea S, Subramanian SV, 2017).

Por medio de estas publicaciones se estimula que investigadores de las ciencias sociales y de las ciencias de la salud, especialmente psiquiatras y psicólogos, hagan uso de herramientas de sistemas que pueden extraer datos, validarlos, analizarlos, verificar su potencia estadística, de la información que la población "sube" a las redes sociales en las diferentes plataformas disponibles. El desafío a instalarse en la comunidad científica podría ser mantener un paradigma de beneficencia y justicia, sabiendo controlar el aumento en el uso de los Big Data en la investigación en salud pública.

Los organismos de Naciones Unidas como OMS muestran interés en *Big Data*. Es parte del Plan de Acción Integral sobre Salud Mental 2013 – 2020, desarrollar y fortalecer sistemas de monitoreo de salud mental. En el documento se hace referencia a la utilización de las plataformas comerciales y a la vigilancia epidemiológica de las enfermedades mentales con especial preocupación por el suicidio.

El uso de la tecnología, de cualquier técnica no es "malo" o "bueno" per se. Depende de intenciones, motivaciones, principios, consecuencias, entre otros factores. Un cuchillo es una herramienta; lo mismo puede servir para partir alimentos y comer, que para torturar y asesinar seres humanos. Así como hay usos adecuados derivados del *Big Data*, también los hay inadecuados (Martin, 2015). Ejemplos abundan. Para algunos los peligros fundamentales giran en torno a la privacidad de los datos personales (Mayer-Schönberger V y Cukier K, 2014). Más

adelante se profundiza en ello en el campo de la salud. Pero no son los únicos riesgos. Puede pensarse que haya a quien le interese tener datos para perjudicar, o al menos, no beneficiar a algunos. ¿Qué tal una compañía farmacéutica que quisiera saber quiénes tienen riesgo de desarrollar alguna enfermedad para los productos que produce dicha compañía? ¿Y las compañías de seguros? Probablemente habría más de una que quisiera tener cuantos datos fuese posible para evaluar riesgos y no asegurar más de un cliente probable. En terrenos que quedan entre lo civil y la salud mental, ¿se podría encontrar por medio de los datos de las personas patrones que predijeran el comportamiento? Philip K. Dick imaginó algo parecido en un relato corto publicado 1956, *The Minority Report* (llevada al cine por Steven Spielberg en 2002). Dick plantea que unos seres mutantes, los "precognoscientes" (o "precogs") pueden ver el futuro. Si el procesamiento de datos asume que la posibilidad predictiva que tienen es efectivamente determinista… se estaría ante un problema serio. Y esto sigue en otras veredas que ya se empiezan a imaginar. Bajo el supuesto de desarrollar robots que puedan encargarse de auxiliar a seres humanos (en salud hay más de una situación donde esto puede pensarse, e incluso no solamente se ha pensado, sino que intenta desarrollarse), los robots tendrían que contar con patrones para tomar decisiones. La cantidad de datos que deberían ser capaces de manejar para crear modelos probablemente predictivos sería enorme. ¿Debería permitirse que un robot tome decisiones solamente con base en esos patrones? ¿Cuáles serían los límites para esa toma de decisiones? De haberlos ¿quién(es) y cómo lo(s) propondrían? Esto lleva al campo que algunos ya denominan como "roboética".

Registro electrónico de datos en salud

El desarrollo tecnocientífico repercute a todo nivel. El desarrollo de sistemas informáticos ha alcanzado los registros en salud, y ha llevado a considerar la problemática ética y legal derivada de esta nueva forma de tratar los datos personales[1]. Sin embargo, a pesar de que la informática lleve algunas décadas de desarrollo, el *Big Data* es realmente un fenómeno hijo del nuevo milenio[2]. Al ser muy reciente, hay muchas cosas que ir esclareciendo y ser muy cautos. Existe un supuesto del cual se parte: que los datos que se analizarán estén completos y que fueron colectados de forma adecuada, esto es respetando los derechos de las personas. Sin este supuesto, no es posible hacer predicciones serias. Esto es de especial relevancia, puesto que la investigación muestra que entre el 4.3% al 86% de los casos la información es incompleta o inexacta en varios campos del registro electrónico (Balas EA, Vernon M, Magrabi F, Gordon LT, Sexton J, 2015). En adelante, en buena medida, la información publicada asume que cuenta con datos completos y correctos para partir de ellos.

La epidemiología digital o detección digital de enfermedades (en inglés DDD, de *digital disease detection*) tiene los mismos objetivos que la epidemiología tradicional, pero con la diferencia de que las fuentes de datos se centran en las electrónicas. Esto trae también un cierto cambio de paradigma, ya que no necesariamente toda la información proviene del sistema de salud. El

[1] Por ejemplo, en el caso de México, en el año 2012 se introdujeron modificaciones a la normativa legal del expediente clínico. Se regula desde entonces a través de la Norma Oficial Mexicana "NOM-004-SSA3-2012, Del expediente clínico", publicada el lunes 15 de octubre de 2012. Muy pronto se tuvo que publicar otra normativa por el registro electrónico, la Norma Oficial Mexicana "NOM-024-SSA3-2012, Sistemas de información de registro electrónico para la salud. Intercambio de información en salud", publicada el viernes 30 de noviembre del mismo año.

[2] Ya se mencionó que el término mismo de *Big Data* surge a finales del milenio anterior, 1999. No es casual entonces, que en la enorme base de datos de PubMed las primeras publicaciones que traten de algún modo temas sobre Big Data inicien en 2003 de modo escaso, en la primera década hayan sido pocas en general, y se hayan multiplicado casi exponencialmente a partir de 2013. Al 17 de agosto de 2017, el número de publicaciones que aparecen en PubMed con el término "*Big Data*" son: 2 en 2003, 1 en 2004, ninguna entre 2005 a 2007, 9 en 2008, 3 en 2009, 2 en 2010, 7 en 2011, y 41 en 2012; en la segunda década el crecimiento muestra un aumento drástico en el número de publicaciones, 201 en 2013, 463 en 2014, 722 en 2015, 1175 en 2016, y en lo que va de 2017 van 898 artículo publicados, lo que hace pensar que se rebasará el número de trabajos de 2016. Hacen falta análisis bibliométricos para apreciar tendencias en estas publicaciones.

caso más reciente ha sido el del Ébola (Anema A, Kluberg S, Wilson K, Hogg RS, Khan K, et al, 2014). Este campo no ha hecho otra cosa más que crecer en el último tiempo (Velasco E, Agheneza T, Denecke K, Kirchner G, Eckmanns T, 2014), lo que ha desencadenado una necesaria reflexión ética al respecto. Se ha considerado que existen tres categorías de problemas éticos en la epidemiología digital (Vayena E, Salathé M, Madoff LC, Brownstein JS, 2015). La primera categoría, "sensibilidad al contexto" contiene los desafíos éticos de: usos en salud pública, usos comerciales de los datos; acuerdos con usuarios, términos de servicio, epidemiología participativa; y aspectos de salud global, en un contexto de protección con nivel elevado. La segunda, "nexos entre metodología y ética", incluye el desarrollo de una metodología robusta con validación de algoritmos, recalibración de tales algoritmos, filtrado de ruido y mecanismos de retroalimentación, así como transparentar la procedencia de los datos. La tercera, "requisitos de legitimidad", incluye la aplicación de estándares óptimos de práctica, promoción y mantenimiento de órganos de supervisión (con políticas de seguimiento permanente y planes de acción para la corrección de resultados falsos), integración de la detección digital de enfermedades con los sistemas de vigilancia estándar, y por último (pero no menos importante) la comunicación constante con la sociedad en su conjunto.

Las categorías precedentes, debieran complementarse una mirada desde la ética en el contexto de protección de las personas, en la necesidad de identificar con claridad la ponderación de riesgos y beneficios del uso de los datos de salud, concretado en las funciones de "*Data Governance*" (Llàcer, MR, Casado M, Buisan L. 2015) entendido como la responsabilidad de los organismos en la gestión de datos que garanticen la seguridad, integridad, transparencia y responsabilidad; lo que finalmente exige la promoción y aplicación de un Código de Ética para la Reutilización de Datos de Salud. En este se requiere la expresión de valores y virtudes que respalden una finalidad ética en la recogida y la utilización de los datos de salud que se obtienen. Además de contar con instancias éticas efectivas que permitan un uso responsable y respetuoso de la información sensible de las personas. El desafío a instalarse en la comunidad científica es mantener un paradigma de beneficencia y justicia, sabiendo controlar el aumento en el uso de los *Big Data* en la investigación en salud pública.

El secreto médico descartado.

Cotidianamente los profesionales de la salud asisten a la incorporación a sus prácticas de nuevos sistemas de registro y almacenamiento de datos, acompañados por propuestas gubernamentales de centralizarlos en el llamado "gobierno electrónico" frente a una creciente sensación de los ciudadanos de pérdida de su intimidad y privacidad, con débiles mecanismos de protección de estos derechos. En el caso de la medicina y su ejercicio, las obligaciones deontológicas de respeto del secreto profesional, están siendo olvidadas, sin mayores reflexiones al respecto, banalizándolas o minimizándolas.
Algunos mitos las atraviesan como el que proclama que la sola incorporación de tecnología produce efectos inmediatos. La efectividad de una organización para diversos fines no es automática, varia según su uso social.

Las tecnologías de la información contribuyen a una mejor asistencia en salud. Facilitan el acceso y mejoran los sistemas de salud. Sin embargo, esta información personalísima requiere de cuidados especiales. Ética, política y tecnología confluyen en la consideración de los derechos humanos. Norberto Bobbio (1982) decía que el problema no son los fundamentos de los derechos sino su protección.

Un ejemplo de esto surge en Ética de la Investigación cuando datos provenientes de registros electrónicos se utilizan con fines de registro de nuevos usos para viejas drogas, proyecto europeo de una plataforma orientada a servicios subyacentes, escalables y adaptables, que, a pesar de las diferentes regulaciones nacionales, permita la reutilización de los datos electrónicos de los hospitales, para efectuar estudios de investigación clínica. Desde el enfoque ético global se involucra a muchos actores importantes de toda Europa para asegurar la aceptación de una metodología de diseño desde los registros electrónicos de pacientes (De Moor G, Sundgren M, Kalra D, Schmidt A, Dugas M, et al, 2015).

Durante el manejo de grandes bases de datos intercambiables y comparables surgen problemas éticos y riesgos de daños colectivos dada la naturaleza cambiante de las relaciones en *Big Data* que no distingue entre prácticas académicas y comerciales (Mittelstadt BD, Floridi L, 2016).

El uso de sistemas de registro y almacenamiento de datos originados en prácticas asistenciales individualizables, intentos gubernamentales de centralizarlos e intercambiarlos con otras agencias en diversas plataformas, plantean cuestiones éticas en relación a información (Rodwin MA, 2009)

Tal vez la cuestión ética central es si los usos secundarios con fines de lucro de datos que no son propios son justificables; y si es así, ¿qué garantías de privacidad deben ser empleadas. (Gostin LO, Nass S, 2009)

La conectividad de las nuevas tecnologías de la información ha dejado a un costado el juramento hipocrático, esa vieja tradición médica de no contar lo que se ha conocido durante el acto médico. Empresas de salud, (estatales y privados), su personal especializado administrativo contable, los proveedores de servicios de atención de la salud, las compañías de seguros, las organizaciones de administración de la salud, los pagadores públicos y privados de atención médica directa y terceros pagadores, requieren el acceso a las historias clínicas personales con distintos niveles de individualización, tanto como agencias gubernamentales, instituciones de salud y otros agentes del Estado. La suma de todo esto ha cambiado completamente al Juramento Hipócratico. (Rothstein MA 2010).

Plataformas, sistemas y "nubes"

A la hora de pensar las bases de datos con información sensible referida a la salud, que puede o no ser susceptible de utilización por parte de entidades privadas, se omite reflexionar bajo que estructuras, sistemas o aplicaciones se esta guardando y compartiendo esta información. La gran mayoría de las estructuras lógicas que albergan esas enormes cantidades de datos suelen pertenecer a entidades también privadas. Sobran casos en los que entidades estatales (ministerios de salud, secretarias, subsecretarias, directorios, coordinaciones o programas y políticas publicas), hospitales, clínicas, laboratorios de análisis clínicos o bancos de sangre utilizan herramientas privadas para albergar y custodiar sus datos. La gran mayoría de estas entidades recurren a software privado para contener esta información. Uno de los casos más actuales es la denominada "Nube". Ya llevamos más de 25 años de Internet a nivel masivo y podemos concluir, que la denominada "nube" no es una entidad neutra, sino que pertenece a empresas que en casi todos los casos tienen acceso directo a esa información. El caso más resonante y corriente es la plataforma Google Drive la cual es utilizada para albergar información por la gran mayoría de las agencias estatales. Esto en parte se debe a la deficiente infraestructura tecnológica estatal o la baja prioridad que se le asigna al desarrollo de plataformas o sistemas propios a nivel público. El valor de mercado de empresas como Google, Microsoft o Apple, por nombrar algunas, está principalmente dado por la cantidad de datos que manejan. Estos datos son útiles para empresas privadas, desde nuestros datos de navegación (que páginas consumimos, que buscamos en la red) hasta que información albergamos en la denominada "nube". Son sobrados los casos de utilización de esta información para vender productos, promocionar campañas políticas (las dos últimas elecciones presidenciales de EE.UU. fueron el campo de batalla de publicidad política derivada de análisis de *Big Data* extraído de redes sociales) o establecer mensajes específicos en los usuarios.

Si bien a nivel normativo, en el caso de agencias públicas, se establece que esos datos deben ser resguardados por las instituciones que los almacenan, nadie controla cuales plataformas utilizan para volcar los datos. Por dar un ejemplo, la gran mayoría de los laboratorios de análisis clínicos utiliza sistemas que, en la gran mayoría de los casos, son proporcionados por grandes laboratorios que los ponen a disposición como parte de la negociación por la compra de equipamiento de análisis y reactivos. De esta manera la información que luego es volcada en el sistema "cedido" queda desprotegida ante los dueños de los sistemas, que pueden hacer uso de esa información para sus propios intereses. Bajo una modalidad similar, pero en un ámbito

de aplicación distinto, la gran mayoría de las políticas públicas recurren a la plataforma de Google Drive o a sistemas de Microsoft para volcar sus datos. Incluso las cuentas de correo electrónico por donde es compartida dicha información también son de desarrollo privado. Actualmente la administración pública de la República Argentina contrató a la empresa Microsoft para la generación de cuentas de correo públicas. De esta manera la información pública queda vulnerable ante los intereses de entidades privadas que puedan hacer uso y abuso de los datos recolectados por la administración nacional.

La vulnerabilidad de los datos queda así expuesta no solamente por falta de protocolos para garantizar la seguridad, sino que también por la propiedad sobre los sistemas o estructuras lógicas en los cuales es depositada esa información, desprotegiendo la privacidad de las personas.

De lo bioético a lo biojurídico

Como se esbozó previamente, la privacidad de datos es un punto crucial; con ello, el proceso del consentimiento informado es un punto crítico para *Big Data* (Rothstein MA, 2015). Las repercusiones no solamente están siendo éticas, sino que empiezan a alcanzar el ámbito de lo jurídico. Dos casos judiciales que involucran la venta de datos de prescripción para la comercialización farmacéutica afectan a la informática biomédica, la privacidad de los pacientes y sus médicos; y la regulación (Kaplan B, 2015). El caso Sorrell vs. IMS *Health Inc.* et al. en los Estados Unidos, y R vs. *Department of Health*, *Ex Parte Source Informatics Ltd.* en el Reino Unido se refieren a la privacidad y la protección de datos de salud, la desidentificación y reidentificación de datos de particulares, la información personal, la privacidad de los clínicos y el deber de confidencialidad, los usos benéficos y desagradables de los datos de salud, la regulación de las tecnologías de la salud y la consideración de los datos como lenguaje. Los individuos deben, cuando menos, ser conscientes de cómo los datos sobre ellos se recogen y utilizan; además, si el proceso del consentimiento es adecuado, deben tener la posibilidad de decidir si se puede disponer de esos datos en un futuro y con qué fines. Teniendo en cuenta cómo se utilizan estos datos, las normas sociales y el derecho deben evolucionar éticamente y en la protección de Derechos Humanos, a medida que las nuevas tecnologías afectan a la privacidad y protección de los datos de salud.

Es bien sabido que la ética no trata de lo que es, sino de lo que debe ser. Si así son las cosas, ¿qué debe hacerse? Como puede verse, los registros de salud electrónicos, el uso compartido de datos, el uso secundario de datos, entre otras materias vinculadas a la información, están permitiendo interesantes oportunidades para mejorar la salud y la atención médica, al tiempo que exacerban las preocupaciones sobre la privacidad. Los dos casos judiciales sobre venta de datos sobre prescripciones ya reseñados, plantean cuestiones de lo que constituye la "privacidad" y el "interés público". Presentan también una oportunidad para el análisis ético de la privacidad de los datos, la propiedad, la mercantilización de los datos. Estos problemas entrelazados implican la discusión de los grandes beneficios y daños del *Big Data*, tocar las dualidades comunes del individuo frente a la colectividad o el interés público, la investigación (o, más ampliamente, la innovación) versus la privacidad, el poder individual versus institucional, la identificación versus identidad y autenticación, así como los individuos virtuales versus los reales y la contextualización de la información. La transparencia, la flexibilidad y la rendición de cuentas son necesarias para evaluar los usos y usuarios de datos apropiados, juiciosos y éticos, ya que algunos son más compatibles con las normas y valores de la sociedad que otros (Kaplan B, 2016).

Desde los mundos ideales hacia el mundo real: responsabilidad ante *Big Data*

Darse cuenta de que hay beneficios y riesgos reales y potenciales ante la realidad del *Big Data* no es suficiente. La ética es una disciplina práctica que interactúa continuamente con el campo jurídico-político, de modo que lo que siempre se desea es dar algún tipo de guía para la acción. De lo contrario, si se queda en el mero nivel de la reflexión, el riesgo de caer en la inacción es grande.

Una propuesta reciente maneja un decálogo que vale la pena analizar desde el punto de vista ético, revisar los enlaces con lo jurídico-político, y estar claros que puede (y debe) modificarse conforme aparezcan más retos y riesgos. El decálogo propone los siguientes puntos para el uso responsable del *Big Data* (Zook M, Barocas S, Boyd D, Crawford K, Keller E, Gangadharan SP, et al, 2017)[3]:

1. Reconocer que los datos son personas y pueden hacer daño.

Problemas previos, tales como la identificación personal y grupal aunados a la estigmatización, toman una nueva dimensión con la posibilidad de la identificación personal, grupal y además, el complemento de la geolocalización. No debe olvidarse que los datos se obtienen siempre de personas, y que aunque los datos no tienen dignidad, pertenecen a alguien que sí cuenta con ella.

2. Reconocer que la privacidad es más que un valor binario.

Si el problema fuese solamente "privado" vs "público", se realizaría una reducción de un espectro que es bastante más complejo. "Privado" tiene más sentidos que solamente el no desvelo en lo público, así como "público" no es que cualquier dato pueda aparecer para los demás. Hay que considerar, en el fondo, espectros en el campo de los datos: cuáles, para qué, quiénes, por qué, etc.

3. Protegerse contra la re-identificación de sus datos.

Probablemente sea uno de los puntos complejos desde el punto de vista técnico, ya que los metadatos asociados son una realidad cotidiana (desde las cuentas de correo electrónico, perfiles en redes sociales, etc., que incluso avisan que los datos los manejan para un "mejor servicio"). De cualquier forma, existe la posibilidad de que se disgreguen datos y que se encripten con fines de protección de los mismos.

4. Practicar el intercambio ético de datos.

Teóricamente, un acceso democrático global sería una luz en el camino a seguir. Conseguir consentimientos, no vender o transferir bases de datos de un particular a otro, limitar la intervención del Estado de forma consensuada con la ciudadanía, etc., serían la base para intercambiar datos de un modo ético.

5. Considerar las fortalezas y limitaciones de los datos; grande (*Big*) no significa automáticamente mejor.

Como se mencionó desde el inicio, sin el supuesto de que los datos están completos para los fines deseados, y que además, son correctos, no hay forma de hacer asociaciones y predicciones moderadamente certeras.

6. Debate sobre las decisiones éticas duras.

Existe una serie de decisiones que deben ser completamente plurales y radicalmente democráticas, con la participación de la ciudadanía (puesto que el *Big Data* implica a todos; hasta las generaciones futuras, ya que cada vez los datos empiezan a asociarse desde las ecografías del control prenatal hacia el futuro). Algunas de estas decisiones deberían considerar, ¿cuál será el papel de los comités de bioética?, ¿cuál será el marco jurídico normativo nacional?, ¿cómo sería la intervención de organismos supranacionales en el *Big Data* de nivel global?, ¿cómo explicitar y limitar los conflictos de interés ante el tratamiento de los datos?

7. Desarrollar un código de conducta para su organización, comunidad de investigación o industria.

[3] La traducción de los diez puntos del decálogo nos pertenece.

Está claro que los códigos de conducta no son mágicos, pero si se construyen entre todos los implicados y todos están dispuestos a seguirlos y hacerlos valer, tienen una fuerza mayor que la mera imposición vertical desde una autoridad.

8. Diseñar los datos y sistemas para la auditabilidad.

La transparencia ética y legal debería ser algo que empiece a construirse ante el *Big Data*. No solamente durante el proceso del consentimiento, sino también y de modo paralelo con la industria farmacéutica, aseguradoras, gobiernos, entre otros. La transparencia debe incluir no solamente los datos que puedan manejarse, sino quiénes los están manejando, por qué, para qué, y por cuanto tiempo.

9. Comprometerse con las consecuencias más amplias de los datos y las prácticas de análisis.

Una persona a quien se le ha seguido desde la ecografía prenatal de control, toda la vida preescolar y escolar con el pediatra, la pubertad y adolescencia con sus redes sociales…[…] ¿en qué momento preguntarle para recabar su asentimiento? ¿Basta el consentimiento de los padres? ¿Por qué? En caso de no estar de acuerdo, ¿habría que destruir los datos? ¿Cómo (bajo el supuesto que ya estuviesen procesados y asociados entre sí y con los de otros usuarios)?

10. Saber cuándo romper estas reglas.

Aunque parece ser contra intuitivo, hay que pensar que al momento actual es lo que puede decirse. Si los derroteros de la investigación sobre Big Data toman otros rumbos, habría que considerar otros temas, otros puntos. Y para ello hay que estar abiertos a no seguir parcial o totalmente alguna de las reglas de esta propuesta de decálogo, eliminar alguna, agregar otra, a la luz de la realidad emergente.

Finalmente, no hay que perder de vista que ante los objetivos del desarrollo sustentable parece ser que los países menos desarrollados tendrían que verse más protegidos del expolio de datos que otros países (Beck EJ, Gill W, De Lay PR, 2016).

Big Data, derechos humanos y protección de datos de carácter personal

Si bien cabe reconocer que el Derecho es reactivo a la realidad social y global, que el avance de las tecnologías es vertiginoso y el crecimiento informático exponencial, la débil regulación de los países facilita el panorama expuesto en la parte principal de este ensayo.

El intercambio de datos personales constituye una realidad imparable y tanto empresas privadas como el propio Estado lo realizan para el desarrollo de sus actividades. Asimismo, las personas físicas voluntaria e involuntariamente, en conocimiento o en ignorancia de los resultados o de los medios de que se valen los proveedores de servicios para obtenerlos, proporcionamos cotidianamente datos de carácter personal, a escala mundial. Salvo la información proporcionada informada y voluntariamente por las personas, los datos personales gozan de protección en el campo del Derecho.

La protección de datos de carácter personal se reconoce en la actualidad como un derecho humano de la tercera generación, con un objeto más amplio que el derecho a la intimidad y vinculado al respeto de la dignidad de las personas. El derecho comprende cualquier tipo de dato personal, cuyo conocimiento o empleo por terceros pueda afectar a los derechos del titular, a quien atribuye el poder de control y disposición sobre estos, el derecho a que se requiera el previo consentimiento para la recogida y uso de sus datos personales, el derecho a saber y ser informado de quién dispone de esos datos personales sobre el destino y uso de los mismos; el derecho oponerse a esa posesión y usos; y el derecho a acceder, rectificar y cancelar dichos datos.

Un tratado abierto a la ratificación de los países es el Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, cuyo objetivo es "garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales,

concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona." (Consejo de Europa, 1981, p. 16). En 2001, se aprobó un Protocolo Adicional relativo a las autoridades de supervisión o control en materia de protección de datos personales y a la prohibición de transferencias internacionales de datos a terceros países u organizaciones que no proporcionen un nivel adecuado de protección; y, en 2016 el Reglamento 679/2016 Europeo de Protección de Datos.

El deber ser apunta a que los países avancen hacia un sistema de tratamiento de datos con seguridad, rendición de cuentas, transparencia, derechos a la información y observancia del principio de proporcionalidad. En resumen, que proteja a sus ciudadanos de abusos en esta materia.

Palabras finales: ¿pensar una ucronía?

No hay que olvidar que la idea de progreso de algún modo es la sustitución secularizada de las promesas de las religiones de una vida futura en otro mundo, al menos en el mundo occidental. Esta idea de progreso ha venido acompañada del desarrollo espectacular de la ciencia y su aplicación tecnológica, de modo que casi es imposible no hablar de la tecnociencia. Además de esta consideración, hay una económica fundamental en estos temas: el sistema económico neoliberal. Analizar datos para ofrecer más y mejores productos de acuerdo con patrones de consumo es la meta para vendedores de productos y prestadores de servicios. Analizar los datos en salud también repercute para la industria, quien estará más pendiente de ofrecer servicios de todo tipo.

Así como una distopía es algo que no tiene un topos, un lugar, una ucronía es algo no sucedido en el tiempo, no tiene espacio temporal. Ante la revolución de los objetos electrónicos conectados, ¿qué habría pasado si no se tuviera la dependencia tecnológica que han alcanzado los seres humanos? ¿qué habría pasado si nunca hubiese aparecido la tarjeta SIM para la telefonía? Se pueden especular muchas cosas que casi por seguro ya no es posible revertir. Parece ser que nadie está dispuesto a dejar de lado la tecnología una vez que la ha probado. ¿Qué responsabilidad nos queda a todos antes este escenario? ¿Cómo estamos participando para que se siga desarrollando?

Referencias Bibliográficas

Anema A, Kluberg S, Wilson K, Hogg RS, Khan K, Hay SI, Brownstein JS (2014). Digital surveillance for enhanced detection and response to outbreaks. The Lancet. Infectious Diseases, 14(11), 1035–1037. http://doi.org/10.1016/S1473-3099(14)70953-3.

Balas EA, Vernon M, Magrabi F, Gordon LT, Sexton J. (2015). Big Data Clinical Research: Validity, Ethics, and Regulation. Stud Health Technol Inform, 216:448-452.

Beck EJ, Gill W, De Lay PR. (2016). Protecting the confidentiality and security of personal health information in low- and middle-income countries in the era of SDGs and Big Data. Glob Health Action, 9:32089. doi: 10.3402/gha.v9.32089.

Bobbio N. (1982). El problema de la guerra y las vías de la paz. GEDISA.

Consejo de Europa. (1981). Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, y Protocolo Adicional 200, Recuperado de http://www.oas.org/es/sla/ddi/docs/U12%20convenio%20n%20108.pdf

De Moor G, Sundgren M, Kalra D, Schmidt A, Dugas M, et al. (2015). Using electronic health records for clinical research: the case of the EHR4CR project. J Biomed Inform. Feb; 53:162-73. doi: 10.1016/j.jbi.2014.10.006. Epub 2014 Oct 18.

Ginsberg J, Mohebbi MH, Patel RS, Brammer L, Smolinski MS, Brilliant L. (2009). Detecting influenza epidemics using search engine query data. Nature, 457:1012-1014

Gostin LO, Nass S. (2009). Reforming the HIPAA privacy rule: safeguarding privacy and promoting research. JAMA, 301(13):1373–1375

Gruebner O, Sykora M, Lowe SR, Shankardass K, Galea S, Subramanian SV. (2017). Big data opportunities for social behavioral and mental health research. Soc Sci Med, Jul 22, pii: S0277-9536(17)30451-3. doi: 10.1016/j.socscimed.2017.07.0-

Kaplan B. (2016). How should health data be used? Camb Q Healthc Ethics. 25(2):312-329. doi: 10.1017/S0963180115000614

Kaplan B. (2015). Selling health data: de-identification, privacy, and speech. Camb Q Healthc Ethics, 24(3):256-271. doi: 10.1017/S0963180114000589

Llàcer MR, Casado M,. Guisan L (coords.) (2015). Barcelona, Bioética y Big Data de salud: explotación y comercialización de los datos de los usuarios de la sanidad pública. en www/bioéticayderecho.ub.edu/publicaciones/documentos

Martin KE. (2015). Ethical issues in the big data industry. MIS Quarterly Executive 14(2): 67-85.

Mashey J. (2017). Big data and the next wave of infrastress. Recuperado de https://www.usenix.org/legacy/publications/library/proceedings/usenix99/invited_talks/mashey.pdf

Mayer-Schönberger V, Cukier K. (2014.). Big Data: a revolution that will transform how we live, work and think. Mariner Books; Boston.

Mittelstadt BD, Floridi L, (2016). The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts, Science and Engineering Ethics, 22, 2, 303

OMS (2013). Plan de Acción Integral sobre Salud Mental 2013/2020 Recuperado de http://apps.who.int/iris/bitstream/10665/97488/1/9789243506029_spa.pdf

Polgreen PM, Chen Y, Pennock DM, Nelson FD. (2008). Using Internet searches for influenza surveillance. Clin Infect Dis, 47:1443-1448

Unión Europea (2016). Reglamento (UE) 2016/679 Parlamento europeo y Consejo, Relativo a la Protección de las Personas Físicas en lo que Respecta al Tratamiento de Datos Personales y a la Libre Circulación de estos Datos, Recuperado de http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

Rodwin MA. (2009). The case for public ownership of patient data. JAMA, 302(1):86–88

Rothstein MA. (2015).Ethical issues in big data health research: Currents in contemporary bioethics. J Law Med Ethics, 43(2):425-429. doi: 10.1111/jlme.12258

Rothstein MA. (2010). The Hippocratic Bargain and Health Information Technology. The Journal of law, medicine & ethics: a journal of the American Society of Law, Medicine & Ethics, 38(1):7-13. doi:10.1111/j.1748-720X.2010.00460. x.

Tribunal Constitucional de España. (2000). Sentencia 292/2000 de 30 de noviembre ECLIS:ES:TC: 2000:292, Recuperado de http://hj.tribunalconstitucional.es/HJ/cs-CZ/Resolucion/Show/SENTENCIA/2000/292

Vayena E, Salathé M, Madoff LC, Brownstein JS. (2015). Ethical challenges of big data in public health. PLoS Comput Biol, 11(2): e1003904. doi: 10.1371/journal.pcbi.1003904

Velasco E, Agheneza T, Denecke K, Kirchner G, Eckmanns T. (2014). Social media and Internet-based data in global systems for public health surveillance: a systematic review. Milbank Q 92: 7–33. doi: 10.1111/1468-0009.12038

Zook M, Barocas S, Boyd D, Crawford K, Keller E, Gangadharan SP, et al. (2017). Ten simple rules for responsible big data research. PLoS Comput Biol, 13(3):e1005399. doi: 10.1371/journal.pcbi.1005399